A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2001-0101-4C

INDEPENDENT STATE AUDITOR'S REPORT
ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS
AND INTERNAL CONTROL DOCUMENTATION AND MONITORING
AT THE DIVISION OF INSURANCE

July 1, 2000 to July 30, 2001

OFFICIAL AUDIT REPORT
DECEMBER 19, 2001

2001-0101-4C

TABLE OF CONTENTS

INTRODUCTION

The Division of Insurance (DOI) was established in accordance with Massachusetts General Laws, Chapter 26, and is one of nine agencies operating under the Office of Consumer Affairs and Business Regulation (OCABR). The Division is managed by a commissioner whose term in office is coterminous with that of the governor. The mission of DOI is to regulate the Commonwealths insurance industry and to license Massachusetts insurance companies, agents and brokers. The Division regulates all aspects of the insurance industry in the Commonwealth. Annually, the Division licenses issues more than 6,200 companies, agencies, and HMOs, and more than 160,000 insurance agent and broker licenses. The Division conducts financial examinations of domestic and foreign insurance companies, audits licensees, reviews rates and policy forms, and participates in rate settings.

The DOI uses information technology extensively to carry out its mission and support its business operations. At the time of our audit, the DOI's information technology infrastructure consisted of a local area network environment comprised of 166 desktop computers, which were configured to run either Windows 95 or Windows 98 and Microsoft Internet Explorer. The Office 97 suite is standard on all microcomputers, with some microcomputers having special application software, such as Attachmate a document handling software, which was available to specific authorized personnel.

All microcomputer workstations at DOI are connected by a 10-megabit Ethernet local area network (LAN). The Division also operates other file servers, including a Banyan e-mail server, a Windows NT domain controller and backup, a Windows 2000 Systems Management Server (SMS), a Windows 2000 Intranet web server, a Windows NT SQL server, a Windows 2000 internet usage monitoring server (Elron), two Windows 2000 file and print servers, a Windows 2000 RAS server and three Windows NT printing queues.

The Division's information technology unit manages the servers, workstations, and access to the various DOI applications. During the past year, the Division in conjunction with OCABR, elected to participate in the statewide MassMail project with the Windows professional version installed on all desktop workstations and servers.

The Division's mission-critical application is the Consolidated Licensing and Regulation Information System (CLARIS). The CLARIS application is a transaction-based system that records information on the insurance companies, agents, and brokers licensed to sell insurance in Massachusetts. In addition, through OCABR, the Division tracks and records revenue generated

from new insurance licensing, as well as renewals processed through the Commonwealth's primary accounting and reporting system known as the Massachusetts Management Accounting and Reporting System (MMARS). The DOI has a dedicated microcomputer to receive information from Fleet Bank with respect to the revenue collected through the bank's lockbox system.

The Division also has connectivity to Massachusetts Access to Government Network (MAGNet) and to the National Association of Insurance Commissioners (NAIC). The Commonwealth's Information Technology Division manages the Internet firewall for the MAGNet and NAIC connections.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

We performed an information technology (IT) audit at the Division of Insurance for the period of July 1, 2000 through July 30, 2001. The audit, which was conducted from January 16, 2001 to September 12, 2001, consisted of an examination of IT-related internal controls pertaining to organization and management, physical security and environmental protection for computer equipment, logical access security, hardware and software inventory, on-site and off-site storage of magnetic media, and business continuity planning. We reviewed data input and output processing activities for the Consolidated Licensing and Regulation Information System (CLARIS). We also reviewed the adequacy of internal control documentation and the sufficiency of internal control-related monitoring activities.

Audit Objectives

The primary objective of the audit was to determine whether adequate controls were in place and in effect for DOI's IT processing environment and whether DOI's internal control structure was adequately documented and monitored.

With respect to IT-related controls, we sought to determine whether adequate IT organization and management controls were in effect to properly support the Division's IT processing environment. We determined whether adequate controls regarding physical security and environmental protection were in place and in effect to safeguard computer operations and IT-related assets. A further objective was to determine whether adequate controls were in place to prevent and detect unauthorized access to DOI's primary application and its data files and to software available through the Division's local area network (LAN) file servers and workstations. Our objective with respect to hardware and software inventory was to determine whether IT-related assets were properly identified, recorded, and accounted for in the Division's inventory records.

We sought to determine whether DOI's business continuity plan would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should a disaster render computer systems inoperable or inaccessible. In conjunction with reviewing business continuity planning, we sought to determine whether proper backup procedures were being performed and whether copies of backup magnetic media were being stored in secure on-site and off-site locations.

With respect to data integrity for the Consolidated Licensing and Regulation Information System (CLARIS), we sought to determine whether adequate input and output controls were in place and whether the system was subject to appropriate access security controls.

With respect to the documentation of internal controls, we sought to determine whether DOI, acting under the auspices of OCABR, had an agency-specific internal control plan and whether documented internal controls were sufficiently comprehensive and detailed to support agency business functions, including IT-related operations. In addition, we sought to determine whether appropriate mechanisms were in place to monitor and evaluate the effectiveness of the agency's system of internal controls.

Audit Methodology

To determine the scope of the audit, we performed a pre-audit survey regarding DOI's IT environment. The pre-audit work included interviews with senior management; a review of policies, procedures, and other internal control documentation; and observation of IT-related areas. To obtain an understanding of the Division's activities and internal control environment, our pre-audit work included a review of DOI's mission, organizational structure, and primary business functions. We assessed the strengths and weaknesses of the internal control system for selected IT-related activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To obtain an understanding and to evaluate the organization and management of IT operations, we reviewed the Division's organizational structure with respect to IT operations and evaluated reporting lines, span of control, unity of command job descriptions, oversight mechanisms, and separation of duties. We reviewed IT policies and procedures to determine the level of documentation regarding the IT general control areas related to our audit.

To determine whether IT-related assets were adequately safeguarded, we reviewed physical security and environmental protection over the microcomputer systems and online workstations through observation, conducting interviews with DOI management and staff, and by completing appropriate audit checklists.

We reviewed DOI's logical access security policies and procedures that should be designed to prevent and detect unauthorized access to the DOI data files and systems on ITD's mainframe and DOI's file servers and microcomputer workstations. We reviewed the security procedures with the MIS Director and the LAN Manager who were responsible for controlling DOI's access to ITD's mainframe, and the Massachusetts Division of Insurance (MA DOI) microcomputer systems. We reviewed the access privileges of those staff who were authorized to access

applications residing on ITD's mainframe, and DOI's IT systems. Subsequently, we determined whether all system users who were authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes. Further, we determined whether users were restricted to only the application programs and data files to which they had been authorized. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted only to authorized users only, we reviewed procedures for authorizing access to DOI's data and system resources on ITD's mainframe, the MA DOI microcomputer systems. We then compared the list of individuals authorized to access DOI's IT systems to the list of current DOI employees to determine whether all current users were employed by DOI.

To determine whether the DOI's hardware inventory record was current, accurate, complete, and valid, we reviewed information on purchased items and compared it to the information recorded on the inventory record, and we conducted verification tests of IT assets from the inventory record to the items and vice versa. We traced a sample of sixty judgmentally selected hardware items to the inventory record to determine whether the hardware items selected were physically locatable, properly tagged, properly recorded, and accounted for with their historical cost valuation. Further, to test whether purchased hardware items were being listed on the inventory records and could be physically located at the DOI, we compared purchase orders and invoices to the inventory record and to actual equipment for twelve items of hardware purchased by the DOI during fiscal year 2000. We compared the state identification numbers listed on the hardware inventory record to the actual equipment on hand.

To determine whether the DOI had implemented adequate controls to account for licensed copies of application software residing on its file servers and microcomputer workstation, we first sought to obtain an inventory list of software installed or available for use. In addition, to determine whether the DOI could ensure that only authorized copies of software were installed on the automated systems, we interviewed the MIS Director regarding procedures used to install and monitor microcomputer-based software, and obtained a current list of authorized software.

To assess the adequacy of business continuity planning, we reviewed the nature and extent of formal planning that would be exercised to resume computer operations in the event that the information technology systems were inoperable or were unavailable. We interviewed DOI management to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place. We reviewed policies and procedures regarding backup media to determine whether appropriate controls were in place to ensure that backup copies of

data files and software would be available should the automated systems be rendered inoperable. Our review of backup procedures included an evaluation of provisions for on-site and off-site storage of critical backup tapes. We also interviewed DOI management responsible for creating backup copies of computer-related media and visited the off-site facility.

To evaluate data integrity for information processed through the Consolidated Licensing and Regulation Information System (CLARIS), we reviewed IT policies and procedures to determine the level of documentation regarding the administration and operation of data input and output processing activities for the CLARIS application. We reviewed the system help wizards designed to guide the user through entering license application for individuals and companies. We reviewed a list of current CLARIS users in the database and their assigned data input profiles and privileges to read, write, edit, and delete data. To determine whether data records contained within CLARIS met data integrity requirements, we reviewed certain reports generated by the CLARIS application and traced data contained within 24 source documents regarding applications and renewals for a sample of licenses to the data contained within the system. We also reviewed error reports, refund processing, and the process of batch printing licenses after output verification.

To determine the existence and appropriateness of internal control documentation, we interviewed senior management at DOI and OCABR, submitted written requests for internal control documentation, and evaluated the internal control documentation received. To assess the nature and extent of the internal control documentation, we reviewed documentation submitted to the OSA and evaluated it against compliance requirements as set forth in Chapter 647 of the Acts of 1989 i.e., The Commonwealth's Internal Control Act. We then requested documentary evidence of internal control monitoring activities to determine whether appropriate mechanisms were in place to monitor and evaluate the effectiveness of DOI's system of internal controls. In this regard, we also reviewed internal control requirements as established by Chapter 647 and the Office of the State Comptroller's Internal Control Guidelines.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) for the United States and generally accepted auditing practices. With respect to IT-related control objectives and controls, we used the Information Systems Audit and Control Foundation's and the IT Governance Institute's *Control Objectives for Information and Related Technology* (CobiT), published in July 2000, to identify IT management control practices as criteria for review.

AUDIT SUMMARY

Based on our audit at the Division of Insurance, we found that there was reasonable assurance that IT-related control objectives would be met with respect to IT organization and management, physical security, hardware and software inventory, and logical access security for the local area network environment and related workstations. While efforts had been taken to address environmental protection, further improvements to strengthen certain controls in this area would provide increased assurance that environmental protection control objectives would be addressed. In addition, we believe that controls should be strengthened in the areas of business continuity planning and on-site and off-site storage of backup media to comply with generally accepted control practices and the Division's established policies and procedures. Our review also indicated that improvements should be made regarding internal control documentation and internal control monitoring.

Our review of DOI's IT-related organization and management indicated that adequate organizational controls were in place and that IT-related policies and procedures were reasonably well documented. We determined that physical security controls in place at the DOI office provided reasonable assurance that IT-related resources would be safeguarded from unauthorized access in as much as the building had security guards, and office entrances and areas housing IT resources were controlled by appropriate security devices. Because the computer room is shared by three entities, we suggest that the primary responsibilities for physical security, environmental protection, and maintenance of the jointly used computer room be assigned and that a final point of accountability be established.

With respect to environmental protection, we found certain controls to be adequate, such as the computer room having fire and smoke detectors, a fire alarm, handheld dry chemical fire extinguishers, an automatic fire suppression system, and a self-contained air filter/dehumidifier and air conditioning unit. However, environmental protection controls could be improved by maintaining an event log for recording environmental problems and monitoring heat and humidity levels; installing visible temperature gauges, water detectors, an emergency shutdown switch; and by hard-wiring the monitoring alarm for the automatic air conditioning unit to a central monitoring location. Understandably, if the alarm were to go off during normal business hours, it is likely that someone would hear it and notify the appropriate parties. However, if the alarm were to engage outside of normal business hours, it is unlikely that someone would be present to hear the alarm and notify appropriate parties. Moreover, although DOI maintains a bank of UPS units in the computer room and additional units in certain wiring closets to help ensure that there

is sufficient continuation of electrical continued power to bring the systems down in a controlled manner under normal circumstances, however, there was insufficient evidence to draw the conclusion that emergency shutdown procedures in off hours, either manual or automatic, were in place to prevent damage to IT resources.

Regarding system access security, we found that documented policies of logical access controls provided reasonable assurance that only authorized users had access to the DOI's primary computer system on which the Division's application systems reside. We found that controls over the administration of user IDs and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should DOI employees terminate employment or incur a change in job requirements. During our audit, nothing came to our attention to indicate that access privileges granted to individuals were inappropriate given their job responsibilities.

Our tests regarding controls over hardware and software inventory indicated that the Division was adhering to documented policies and procedures and was conducting periodic physical inventories. Our tests indicated that hardware items were locatable, properly accounted for and tagged, and that software products were accounted for and in accordance with licensing agreements.

With respect to system availability, we found that DOI had a documented business continuity strategy and disaster recovery plan. Although the plan appeared to reflect an appropriate strategy on paper, adequate business continuity controls were not being exercised to provide reasonable assurance that systems could be recovered in an acceptable period of time. At the time of our audit, we found that backup copies of magnetic media of data files were not being stored off site in accordance with DOI's policies. Rather than having the backup copies stored at the designated off-site location, they were ostensibly being stored at an employee's home. In addition, although the plan had been executed to a certain degree to regain processing capabilities due to a loss of power resulting from a fire, recovery and contingency plans had not been subject to comprehensive testing and subsequent review. From a risk mitigation perspective, DOI would benefit from having documented emergency shutdown procedures performed in a test made by IT staff during normal business hours or by other designated staff during off hours, to prepare for an emergency or disaster. In addition, documented procedures were not in place to ensure that business continuity plans would be tested and reviewed for their continued viability given changes in technology, staffing, business requirements, or risks to the processing environment. Although appropriate procedures were in effect for generating backup copies of magnetic media, storage of on-site and off-site backup tapes needed to be strengthened to provide improved

physical security and environmental protection controls and sufficient accounting of backup media stored on and off site.

With respect to off-site media storage, DOI's MIS Director stated that the backup tapes were taken to an employee's home on weekends and not to a site designated in DOI's procedures. Because the off-site storage area was a private residence, it was not subject to management review and approval or independent verification that appropriate controls were in effect to safeguard the backup media. As a result, we were unable to confirm that appropriate physical security and environmental protection were afforded to DOI's backup media stored off-site. In addition, there was no documentation to verify that backup copies were stored off site and to indicate which tapes were stored at the off-site location. We believe that DOI's initial intent to have backup media stored in an off-premises state facility is a better strategy in that it does not unfairly place certain responsibilities on an employee and would provide for a site where controls can be tested and reviewed. We recommend designating an off-site area for the proper storage of back-up media, implementing improved inventory control over backup media, and establishing sign-in and sign-out log for the computer room and off-site storage area. We further recommend that DOI evaluate the need to store backup copies of hard copy documents that would be difficult to replace in a secure off-site location, either in hard copy or electronic form in order to enable DOI to restore this information should a disaster destroy on-site copies.

With respect to data integrity, we found that DOI had adequate policies and procedures regarding the administration and operation of data input and output processing activities for the CLARIS application. Our review of CLARIS users' access accounts indicated that appropriate levels of access privileges were assigned for user's job titles and responsibilities. Finally, our review found no discrepancies in information and reports generated through the CLARIS application when comparing information in the system's data files to source data contained in a sample of 24 original source documents, which included applications and renewal forms for various licenses.

Regarding our review of DOI's internal control policies and procedures, although we were provided elements of internal control policies and procedures and although DOI and OCABR appeared to have adequate procedures in place to control revenue and income, license renewal processing information, and insurer and agent licensing activities, we were not provided with a current, sufficiently comprehensive and cohesive, agency-specific internal control plan for DOI. Based on the internal control documentation reviewed, IT-related controls examined, and interviews, sufficient evidence was not provided to demonstrate an adequate level of internal control monitoring and evaluation.

AUDIT RESULTS

1. Internal Control Documentation, Monitoring, and Evaluation

Our review of DOI's internal control documentation revealed that although the Division did have documented internal control policies and procedures and an OCABR-designated internal control plan, DOI could not readily provide an agency-specific internal control plan that detailed internal controls in place to address DOI's administration and business operations. We believe that DOI did maintain policies and various sets of operating procedures to cover its business functions, but that the policies and procedures were not assimilated either by content or by cross-reference into a formally-documented, comprehensive, and cohesive agency-specific internal control plan to cover DOI's twelve divisions.

Chapter 647 of the Acts of 1989, an act relative to improving internal controls within state agencies requires "internal control systems of the agency are to be clearly documented and readily available for examination. Objectives for each of these standards are to be identified or developed for each agency activity and are to be logical, applicable, and complete. Documentation of the agency's internal control systems should include (1) internal control procedures, (2) internal control accountability systems, and (3) identification of the operating cycles. Documentation of the agency's internal control systems should appear in management directive, administrative policy, and accounting policies, procedures and manuals."

Furthermore, based on our review of the internal control documentation provided and the IT-related control areas covered in this audit, we believe that DOI did not perform a comprehensive monitoring and evaluation function to determine whether internal controls were operating as intended to meet established operational and control objectives. Although the DOI did have limited internal controls to provide reasonable assurance that management and primary business objectives were in conformity with its mission, the Division maintained only an informal monitoring or internal control function occurring through informal meetings. Furthermore, although the OCABR internal control staff stated that meetings were held between DOI and OCABR to monitor internal control practices, we were unable to verify whether minutes were maintained for these meetings or to determine whether the topics being discussed were sufficient to support an actual monitoring and evaluating function.

While the Division was responsible for the development and exercise of an appropriate internal control structure, including internal control documentation, to provide reasonable assurance that operational and control objectives would be addressed, we recognize that DOI was

partially dependent on its governing agency, OCABR, for internal control guidance and documentation. It appears that the Division has used OCABR's operations staff to address what were often internal audit or monitoring functions. Due to the increase in operational activity through OCABR for nine separate state agencies, increased emphasis on improving internal control documentation and monitoring is warranted. In particular, to strengthen the overall framework of control, risk analysis should be performed and control metrics should be established for each business activity covering the nine agencies. Also DOI must be responsible for documenting its own monitoring and evaluating activities to assure that the internal controls in place are functioning in the manner prescribed by management.

There are various sources that DOI can reference to assist in developing control self-assessment and monitoring and evaluation techniques, such as the "Internal Control Guides" from the Office of the State Comptroller and the "Internal Control – Integrated Framework" document from the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. With respect to providing an independent internal review function, additional guidance is provided in the Codification of Auditing Standards AU Section 322.02, which notes "Internal Auditors often perform a number of services for management, including, but not limited to, performing tests of controls, reviewing operating practices to promote increased efficiency, and making special inquiries at management's direction." In addition, the work performed by the internal auditors supplements the work performed by the external auditors as noted in Section 322.04 of the code, which states "The work performed by internal auditors may be a factor in determining the nature, timing, and extent of the independent auditor's procedures. If the independent auditor decides that the work performed by the internal auditors may have a bearing on his own procedures, he should consider the competence and objectivity of internal auditors and evaluate their work."

Our conclusions, based on our audit work, were that internal control documentation was not sufficiently comprehensive and that routine monitoring and testing of the Division's system of internal controls did not always occur or was not adequately documented. As a result, the Division cannot be adequately assured of consistently implemented and applied policies and procedures without having a fully-integrated monitoring and evaluation activity in place. We believe that the volume of activity, which in some years exceeds $60,000,000 annually for DOI and with the processing of various business activities through DOI and OCABR, warrants implementation of a formal monitoring and evaluation process and consideration of an internal audit function in conjunction with OCABR to assess the efficiency and effectiveness of DOI operations and internal controls.

Recommendation:

The DOI, in conjunction with OCABR, should strengthen their internal controls documentation by developing a comprehensive and cohesive agency-specific internal control plan. We suggest that DOI identify all sets of documented procedures that address operational and control objectives for separate business functions. We recommend that DOI establish a framework for its internal control plan to which existing sets of internal documentation can be cross-referenced. The internal control plan should include administrative, accounting and operational control procedures covering the business activities performed by the various divisions at DOI.

We recommend that DOI also strengthen its internal control practices by performing risk analysis on a periodic basis sufficient to identify business and operational risks that need to be addressed by internal controls. We recommend that DOI, in conjunction with OCABR, establish appropriate mechanisms to monitor and evaluate the effectiveness of internal controls. The latter would include mechanisms to measure whether controls are operating as intended and developing control self-assessment processes where appropriate. The DOI, in conjunction with OCABR, should define the responsibilities of an internal control officer as required by the Office of the State Comptroller.

Auditee's Response:

> *As the audit report indicated, the OCA&BR directly manages all budgetary, accounts payable, accounts receivable, payroll and human resource activities for the DOI and its eight sister agencies. The report indicated that we had adequate procedures in place to control revenue and income, license renewal processing information, and insurer and agent licensing activities, but that the corresponding documentation for other DOI activities was disjointed and not easily accessible. The DOI is participating in the Risk Assessment and Internal Control program recently established by the Comptroller's Office. We have sent staff to training and have completed the identification of agency-wide risks. During this process, we confirmed that we in fact have internal controls in place to mitigate these risks, although we would agree with the auditors, that constructing a single document would be a valuable project. Currently, we are collecting and correlating our existing documentation with a view toward the creation of such a single agency wide internal control document that will include the testing and evaluation activities that need to be performed. Once completed, it is our intention to place this document, with the appropriate links, on the OCA&BR and DOI intranets so that it is easily accessed by all employees.*

Auditor's Reply:

Documentation of policies and standard operating procedures are an essential component of an internal control structure, along with documentation of business processes and supporting systems and the record of activity for each system. However, once a comprehensive and cohesive internal control plan for DOI is developed, it is essential to set up monitoring and evaluating mechanisms to ensure that internal control policies and practices are in effect to provide reasonable assurance that operational and control objectives will be met.

2. Business Continuity Planning

Although DOI had developed a recovery strategy for applications residing on its LAN file servers and networked microcomputer workstations should processing capabilities be lost, we determined that DOI, in conjunction with OCABR, had not fully tested its business continuity plan for restoring computer functions in the event of a substantial loss of IT operations. With regard to the availability of backup, we found that provisions for controlling on-site and off-site storage of backup media needed to be strengthened.

We acknowledge that DOI was aware of the need for business continuity planning, had documented procedures for on-site and off-site storage of backup media and had a documented recovery plan. Although DOI indicated that they had been forced to test their plan when they had to recover from a loss of electrical power resulting from a fire in their building and that they successfully recovered their IT operations, the plan has not been updated or undergone comprehensive tests to address other disaster scenarios. Since the IT infrastructure has been changed since this particular recovery effort, additional review and testing should have been performed to assess the business continuity plan's viability. Further, evidence was not available to indicate that the plan had undergone detailed walk-throughs of the recovery strategies for different disaster scenarios, nor were any test results available for review.

A business continuity plan should document the DOI recovery strategies with respect to various disaster scenarios. Without a formal and tested recovery strategy for the file servers and stand-alone microcomputers, DOI might experience delays in reestablishing the processing of mission-critical information. The lack of a detailed, tested plan to address the resumption of processing by the LAN and microcomputer systems might render DOI's data files and software vulnerable should a disaster occur. If the LAN or microcomputers' hard drives were damaged or destroyed, DOI could lose critical, important, and confidential data, including insurance licensing and rating information not yet included on backup media.

The objective of business continuity planning is to help ensure the continuation of mission-critical functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted business practices and industry standards for computer operations support the need for each entity to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans. To that end, the DOI should assess the extent to which it is dependent upon the continued availability of IT systems for all required processing or operational needs and develop its recovery plans based on the critical aspects of its information systems.

The DOI, in conjunction with the OCABR should perform a risk analysis of the systems and data to clearly understand the impact of lost or reduced processing capabilities and loss of hard-copy files.

Although DOI was maintaining on-site backup magnetic media, we found that the copies of on-site backup media were left on top of IT equipment and not stored in a secure and environmentally sound fashion. Although DOI had made a good-faith effort to address off-site backup storage of computer media, security over backup copies stored off-site could not necessarily be assured during our audit because the copies of backup tapes were stored at an employee's residence contrary to DOI's policies designating another off-site storage location. The practice of storing backup copies of computer media at employee's home places certain expectations on the employee regarding security over backup media which may be difficult to adequately ensure and that would be impractical to review and test. For example, it may be difficult to obtain sufficient assurance that appropriate controls are in effect to ensure that the backup copies are adequately safeguarded and accessible to only authorized personnel. Furthermore, employees are unfairly placed at potential liability should the backup data file be lost or stolen or should confidential data be disclosed. While off-site storage was supposedly being provided, we could not confirm that backup copies were stored off site and that appropriate controls were in effect to account for and safeguard backup media.

Recommendation:

We recommend that management, in conjunction with OCABR and key users, thoroughly review their business continuity strategy for comprehensiveness and viability for all mission-critical and essential systems. The DOI should ensure that adequate user area plans are in place to ensure that business processing capabilities can be restored, should IT operations be rendered inoperable or inaccessible. We recommend that the business continuity plan be updated as

needed to reflect the current IT infrastructure and be thoroughly tested to the degree possible. We recommend that test scripts be defined and that test results be adequately documented and reviewed by management and business process owners.

Once the business continuity plan has been formally accepted and tested, the plan should then be periodically reviewed and updated to address changes in technology, staff, business conditions or risks to the IT environment. The DOI should specify the assigned responsibilities for maintaining the plans and supervising the implementation of the tasks documented in the plans. The DOI should specify who should be trained in the implementation and execution of the plans under each of the noted disaster scenarios and who will perform each required task to fully implement the plans. Further, copies of the completed business continuity and user area plans should be distributed to all appropriate staff members. A copy of the plans should also be kept in a secure, off-site location.

With regard to on-site storage of backup media, we recommend that DOI store their on-site backup media in a secure and environmentally sound manner. With regard to off-site storage of computer media, we recommend that the Division follow their established policy in using another state agency under OCABR's management umbrella. We recommend that DOI store their off-site backup media in an adequately controlled facility outside of the building within which DOI is located. Finally, DOI should document and monitor the process of generating, storing and retrieving backup media at on-site and off-site locations. The latter should include inventory control, sign-in and sign-out procedures and proper maintenance and use of the tapes.

Auditee's Response:

During the time the auditors were on site, the DOI was migrating from Banyan to Windows 2000. Our documented recovery plan had not been updated to fully reflect the new operating environment. Today we have in place a system that takes our Windows 2000 data off site in an orderly fashion. Additionally, our parent agency, OCA&BR, which is over 2 miles away from One South Station, is separately backing up the Domain controllers. The DOI acknowledges that its interim use of off-site storage for the Banyan System was informal, but it was also a practical short-term solution. With our new operating system, we have defined a complete cycle as part of our infrastructure changes from Banyan to Windows 2000 servers.

Additionally, the DOI has undertaken a risk assessment of its mission critical commitments and has determined that should it experience a situation that prevents the staff from physically accessing the site or should our records be destroyed, we could still meet our obligations.

Insurance is regulated state by state with all states accessing an electronic copy of its domestic companies' financial statements from the National Association of Insurance Commissioners ("NAIC") National Data Base. The advantage of this system is that should the MA DOI be unable to access its computer information, we could go to another state in our region to access the information on the NAIC database. This system has been tested recently. The events of September 11th displaced the NY insurance department from their offices. They accessed the financial records they needed by placing staff in neighboring states' insurance departments. An added benefit of our new operating environment is that it places us under an OCA&BR domain. As such the DOI can access its network from any of its eight sister agencies, its parent, or ITD. Because DOI is part of the state "forest" an authorized member of our staff or a domain administrator can access our servers from any location within the "forest" and shutdown servers in an emergency. The process of emergency shutdowns, both locally and remotely, is being developed and added to our operations manual and, if applicable, to our business continuity plan. We therefore believe that we have thought through the risks and identified contingency plans. What remains is for the MA DOI to independently test this contingency plan. We thank the auditors for this recommendation.

Auditor's Reply:

We concur with the Department's approach regarding the development and formal documentation of a comprehensive business continuity strategy. In addition to formal testing of the plan, once developed and documented, the business continuity plan should be periodically reviewed and updated to reflect changes in operation, personnel, and information technology should be appropriately trained.

Additional Auditee's Response:

> *As you are aware, the DOI shares day-to-day management of the Computer Room with two of its sister agencies (DOB and DTE) with oversight from our parent, OCA&BR. DOI assumes responsibility for most local facility issues because its MIS group is physically adjacent to the Computer Room. There is an informal communication structure between and among the three line agencies that has been mutually beneficial. We agree that while this informal structure has worked, it needs to be formalized and are working with our sister agencies and our parent agency, OCA&BR to produce a document that formalizes our current processes.*

Auditor's Reply:

We agree with DOI's planned actions to ensure proper controls for the jointly used computer room.